REMARKS

Applicants respectfully request reconsideration of the present application based on the foregoing amendments and following remarks. By this Amendment, claims 1, 2, 14, 15, 27 and 28 have been amended. Upon entry of this Amendment, claims 1-28 will remain pending in the application.

Supplemental Amendment

Applicants filed a responsive amendment on November 21, 2006. This paper is intended to supercede and replace that responsive amendment. Applicants respectfully request withdrawal of the previously filed amendment in lieu of this filing.

Objections to the Claims

Claims 6 and 19 stand objected to for informalities. Applicants respectfully disagree with the basis for this objection. The Office Action states the claims should be amended to be "consistent with the specification." Specifically, the Office Action proposes changing "key administrator" in the claims to "key generator administer [sic] and certifier," which is the specific name of an example element described in the specification. Although Applicants agree that this element described in the specification is one example of how the inventions of claims 6 and 19 can be practiced, the claimed inventions are not limited by examples in the specification. Accordingly, Applicants elect to use the broader term "key administrator" which, as the Office Action notes, can have example aspects as described in the specification in connection with the key generator administrator and certifier (KGAC). The claim term "key administrator" is not inconsistent with the specification term "key generator administrator and certifier," it is just broader. Accordingly, the objection should be withdrawn.

Claim Rejections Under 35 U.S.C. 102

Claims 1-5, 9-18 and 22-28 stand rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,920,561 to Gould et al. ("Gould"). For reasons set forth more fully below, this rejection is respectfully traversed.

Amended Independent Claims 1, 14 and 27 Patentably Define Over Gould

Amended independent claim 1 sets forth a method for providing authentication for secure transactions. It requires, inter alia, (a) collecting a biometric sample from a user associated with a request for access to a service, (b) comparing the biometric sample to a biometric template associated with the user, and (c) if the comparison results in a match: (c1) encrypting the request with a private key without providing the private key to the user and (c2) providing the service with access to a public key corresponding to the private key.

Accordingly, amended independent claim 1 clearly requires that the private key is only used following a successful comparison of a biometric sample collected from the user and a biometric template that is associated with the user and encrypting the user's access request with a private key without providing the private key to the user.

Gould does not teach or suggest the invention of amended independent claim 1. Gould teaches a "free seating" system where a user can use any client computer in a network to access the network. (Title) The client computers include a biometric scanning device to obtain samples from the user. (col. 5, lines 14-17) Each client computer already has its own unique private key that is automatically provided to the user. (col. 5, lines 19-21). After obtaining the user's sample and before the user is verified the user encrypts the sample with the client computer's private key and sends the encrypted sample to the server. (col. 5, lines 22-23). Clearly, the user of Gould's system does not need to do anything to get access to the private key apart from sitting at the computer. And Gould does not describe any other private keys that are provided to the user or used by the user or server. Accordingly, Gould does not teach or suggest at least the requirements of claim 1 of only using a private key if there is a successful match between a collected biometric sample and a stored template and encrypting an access request while not providing the user with the private key used to encrypt the request.

For at least these reasons, independent claim 1 patentably defines over Gould. Independent claims 14 and 27 have been amended to include similar subject matter as that highlighted above for claim 1, and so they also patentably define over Gould for at least these reasons. Accordingly, the 102 rejection of claims 1, 14 and 27, together with claims 2-5 and 9-13 that depend from claim 1, claims 15-18 and 22-26 that depend from claim 14, and claim 28 that depends from claim 27, should be withdrawn.

The Dependent Claims Further Patentably Define Over Gould

All of the remaining rejected claims depend from independent claims 1, 14 and 27 and are patentable for at least the reasons presented above. Nevertheless, the dependent claims recite subject matter that still further patentably define over Gould.

Claims 3 and 16 require providing the digital signature that is generated per claims 2 and 15 to the service associated with the request. Gould's signature generated in step 416 is just provided back to the user, not to a service that the user is requesting. Accordingly, Gould does not meet the explicit limitations of claims 3 and 16.

Claims 4 and 17 require providing a biometric signature corresponding to the biometric sample to the service associated with the request. Gould's signature generated in step 416 is just provided back to the user, not to a service that the user is requesting. Accordingly, Gould does not meet the explicit limitations of claims 4 and 17.

Claims 9 and 22 require including integrity information in an encrypted biometric sample that is collected for transmission to an authentication server. The Office Action merely points to a signature sent with an encrypted sample. There is no information included in the sample, much less integrity information as required by the claims. Accordingly, Gould does not meet the explicit limitations of claims 9 and 22.

Claims 10 and 23 require decrypting and checking the integrity information that is included and encrypted in claims 9 and 22. Gould's server 100 merely checks signature information that is sent with a collected sample, not integrity information in the encrypted sample. Accordingly, Gould does not meet the explicit limitations of claims 10 and 23.

Claims 11 and 24 require that the integrity information of claims 9 and 22 includes a unique transaction identifier. The Office Action correctly fails to point to any such identifier. Accordingly, Gould does not meet the explicit limitations of claims 11 and 24.

Claims 12 and 25 require associating user identification information with the private key that is provided to the user depending on the biometric sample match. Claims 12 and 25 further require maintaining a certificate containing the user identification information. The Office Action points to Gould's database of user's biometric templates and user credentials that are sent to the client computer. However, the templates and credentials are not associated with a private

key that is provided to a user as required by the claims. Accordingly, Gould does not meet the explicit limitations of claims 12 and 25.

For at least these additional reasons, the dependent claims further patentably define over Gould and the rejections thereof should be withdrawn.

Claim Rejections Under 35 U.S.C. 103

Claims 6-8 and 19-21 stand rejected under 35 U.S.C. 103(a) as being obvious over Gould. For reasons set forth more fully below, this rejection is respectfully traversed.

Claims 6-8 depend from claim 1, and claims 19-21 depend from claim 14. Claims 1 and 14 have been shown above to be patentable over Gould because at least two elements required by the claims are completely missing from Gould. Accordingly, there is no prima facie case of obviousness against claims 1 and 14 either, and so the subject matter of claims 6-8 and 19-21 is not obvious in view of Gould for at least this reason.

Moreover, Applicants respectfully disagree with the bases supplied in the Office Action for these rejections.

Claims 6-8 and 19-21 define explicit requirements for a pre-enrollment process, including requirements for generating a final enrollment key, verifying registration of a user before creating a biometric template, and associating user information with a final enrollment key. Gould says nothing whatsoever about an enrollment process, or verification of users before a biometric template is created. Gould merely states that a biometric template for an employee is typically created when the employee is initially granted access to the system (col. 5, lines 28-31). Still further, it is not believed appropriate for the Examiner to take Official Notice of the entire contents of six claims based on a mere familiarity with store credit cards. For example, claims 6-8 require: (a) generating pre-enrollment keys for the user; (b) supplying the pre-enrollment keys to respective key generators; (c) generating a final enrollment key for the user only if keys provided by a key administrator match the pre-enrollment keys supplied to the key generators, the key administrator being a person different than the key generators; (d) verifying registration of the user in accordance with a comparison of the final enrollment key; (e) creating the biometric template for the user only if registration is verified; (f) generating the private key only if the biometric template is successfully created; and (g) associating user identification

information with the final enrollment key. This subject matter is explicitly required by the claims and is not required in a department store credit card issuing scenario as described in the Office Action.

For at least these additional reasons, the 103 rejection of claims 6-8 and 19-21 should be withdrawn.

Double Patenting

Claims 1, 13, 14, 26 and 27 stand provisionally rejected on the ground of nonstatutory obviousness-type double patenting in view of claims 1, 17, 18, 20, 36, 39 and 44 of co-pending application 09/801,468 ("the 468 Application"). For reasons set forth more fully below, this rejection is respectfully traversed.

The below table compares the claims identified in the present application as being rejected, along with the claims from the '468 Application which appear to be relied upon for the rejections.[1] As can be seen from the table below, there are many elements in the present claims that are completely missing in the '468 Application claims, and vice-versa.

Present Application	'468 Application
1. A method comprising:	1. A method for reducing the occurrence of unauthorized use of on-line resources, comprising:
receiving a request for access to a service;	receiving a message indicating a request from a user to use on-line resources;
	determining whether the request requires authentication;
collecting a biometric sample from a user associated with the request;	obtaining an indicia of physical identification from the user if authentication is required;
comparing the biometric sample to a biometric template associated with the user;	comparing the obtained indicia to a stored indicia for the user; and

[1] The '468 Application claims have been amended, and should include even further elements that are not found in the present claims. However, it is believed that these claims as filed in the '468 Application are sufficiently distinctive to eliminate the basis for the rejection.

Present Application	'468 Application
if a result of the comparing step indicates a match: **encrypting the request with a private key, wherein the private key is not provided to the user**, and **providing the service with access to a public key corresponding to the private key.**	enabling the request to be fulfilled if the obtained indicia matches the stored indicia
13. A method according to claim 1, wherein the biometric sample includes a fingerprint scan.	17. A method according to claim 1, wherein the indicia is a biometric.
	18. A method according to claim 17, wherein the biometric is one or more of a fingerprint, a voiceprint, a palmprint, an eye scan, and a handwriting sample.
14. An apparatus comprising: means for receiving a request for access to a service; means for collecting a biometric sample from a user associated with the request; means for comparing the biometric sample to a biometric template associated with the user; if a result of the comparing means indicates a match: **means for encrypting the request with a private key, wherein the private key is not provided to the user**, and **means for providing the service with access to a public key corresponding to the private key.**	20. An apparatus for reducing the occurrence of unauthorized use of on-line resources, comprising: means for receiving a message indicating a request from a user to use on-line resources; **means for determining whether the request requires authentication;** means for obtaining an indicia of physical identification from the user if authentication is required; means for comparing the obtained indicia to a stored indicia for the user; and means for enabling the request if the obtained indicia matches the stored indicia

Present Application	'468 Application
26. An apparatus according to claim 14, wherein the biometric sample includes a fingerprint scan.	36. An apparatus according to claim 20, wherein the indicia is a biometric.
27. An authentication infrastructure comprising: a server that intercepts requests for access to a service; and a client that collects a biometric sample from a user associated with the request, wherein the server maintains a biometric template associated with the user for authenticating the collected biometric sample, and wherein, if the collected biometric sample matches the biometric template: **the server encrypts the request with a private key, so that the user need not maintain a token for accessing the service, and the user need not receive the private key**, and **the server provides the service with access to a public key corresponding to the private key**.	39. An apparatus for reducing the occurrence of unauthorized use of on-line resources, comprising: a server that is adapted to communicate with a network based service so as to receive a message indicating a request from a user to use the network based service; **a rules subsystem coupled to the server that determines whether the request requires authentication,** and causes the server to obtain an indicia of physical identification from the user if authentication is required; and an authentication subsystem coupled to the server and the controller that compares the obtained indicia to a stored indicia for the user, wherein the server sends a signal to the network based service that the request is to be fulfilled if the authentication subsystem determines that the obtained indicia matches the stored indicia. 44. An apparatus according to claim 39, wherein the indicia is a biometric, the apparatus further comprising a **database that stores a plurality of biometrics for a respective plurality of users**

As can be clearly seen, there are multiple elements that are not included in the claims of the two commonly-owned applications, and so there is no prima facie support for the proposition

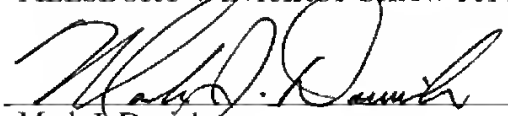
that they are obvious in view of each other based on only the teachings of the claims themselves. Accordingly, the double patenting rejection should be withdrawn.

Conclusion

All objections and rejections having been addressed, the application is believed to be in condition for allowance and Notice to that effect is earnestly solicited. If any issues remain which the Examiner feels may be resolved through a telephone interview, s/he is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,
PILLSBURY WINTHROP SHAW PITTMAN LLP

Date: November 29, 2006



Mark J. Danielson — 40,580 Reg. No.
(650) 233-4777
Please reply to customer no. 27,498